Cellular Fraud Runs Wild!

Ringing Up a Costly Nightmare

BY HAROLD ORT, N2RLL

Every minute of every day someone gets ripped off. Always has been, always will be. Theft takes many forms, and depending on your viewpoint, you're either the thief or the victim.

Certainly most of us would agree that the government rips us off; whether it's in the form of taxes or excess road tolls. Then there's all the commercial gyps, from overpriced medical care to outrageous costs for food and utilities.

Of course if you ask the car manufacturers they'll have reasons for passing on the cost, the tax man definitely has reasons, and so does your friendly cellular carrier. With everyone blaming everyone else, we're stuck in the middle holding the bills.

Never fear, though. There's still a chance you'll get a good night's sleep because according to the Cellular Telecommunications Industry Association, typically one arrest is made daily in the war against cellular fraud, a war where every day criminals ring up more than $1.32 million in fraud. CTIA Fraud Task Force chairman Tom McClure said 40,000 illegal numbers are activated monthly. Unfortunately cellular fraud is seen moving from the hacker to organized crime and drug traffickers.

Just what is cellular fraud and why the fuss over how much is lost every year on this crime—a crime that goes unnoticed by most of us; but yes, you guessed it, one way or another someone pays for the rising administrative costs of policing cellular fraud. In 1993 alone, more than $365 million was lost to cellular fraud which is defined as the act of obtaining cellular service by fraudulent means to avoid paying for the service. Last year a whopping $482-million was lost.

At first thought, it might seem easy to catch these criminals, but as Cellular One of New York and New Jersey points out, in the past two years alone, the industry has spent more than $7-million fighting the crime. "However," they said, "almost as fast as anti-fraud technology can be developed, criminals are finding new and innovative ways to cheat consumers."

Interestingly it isn't always drug traffickers and felons using cloned cellular technology, it's sometimes everyday folks who get caught in a web of trying to save a buck. Take for example the store "fronts" that will sell you a phone service. You won't be able to receive calls, but you can sure make plenty of them, for a price, of course.

Every time you talk over your cellphone, your number is on line for crooks.

But that price is typically much less than the legal way most of us do business!

Cellular fraud is nothing new. Ever since the first cellular phones went on the air, cellular fraud has increased at near epidemic rates. Frankly, one source said the industry was counting on the belief that no one would figure out how to reprogram the phones for illegal use. Oops, someone goofed big time!

Four Basic Types of Cellular Fraud

With more than 14,000 new cellular customers every day, our mobile society has adopted the cellphone—mobile, portable, and transportable—as the latest in stay-in-touch technology to keep users and their families safe, secure, and business-savvy. Of course where there's a buck to be made, unsavory characters will be there with their hands in your wallet. Here's what these criminals do.

First, there's "access fraud" which involves the tampering, programming, and unauthorized use of a cellphones' mobile ident number (MIN), and 11-digit electronic serial number (ESN)—the fingerprint of your phone. Every time you place a cellular call, these numbers, unique to your phone, are transmitted to the carrier's switch station for validation. These codes can be duplicated and then programmed into another phone. This counterfeiting or "cloning," is very common and most frequently used.

When your cellular phone is using another carrier system outside your home service area, you're "roaming." When a cellular thief changes your ESN and MIN after each call while he's roaming, this "tumbling" confuses the cellular switch just long enough to make and complete a call—most likely a lengthy, long distance call!

Subscription fraud is also common—someone subscribes to cellular service using phony identification and other fraudulent information. The industry continues to improve its verification process and credit checks to eliminate this type of fraud.

Another somewhat easier-to-discover type of fraud is stolen phone fraud. As the name implies, someone steals a valid subscriber's cellular phone and makes numerous calls—usually long distance—before service is denied.

Then there are the infamous call-sell scams. This is the typical "cash per call" scam that involves reselling cell telephone services obtained through any of these fraudulent methods. Usually conducted on the street or in apartments, it attracts folks who want to make international long distance calls, such as illegal immigrants or drug traffickers. Last year Baltimore's Bhardwaj Esau was sentenced to 27 months in a federal prison, and his accomplice, Enayet Hussain Ahmed got seven months after being convicted of this call-

Cellphones can have their identities stolen by crooks who use them in cloned phones.

sell scam. In just a two day period they stole thousands of dollars of cellular airtime.

Tough Times for Criminals

Everyone agrees that this high tech war deserves high tech weaponry, and that's exactly what the industry is using. So, with all the criminals out there and technology at their fingertips, how successful is the industry at nabbing the bad guys? Bell Atlantic Mobile's in-house Fraud Task Force is using the most sophisticated Fraud Detection System in the country to pinpoint fraudulent calling activity and lead law enforcement officials to criminals for arrest. The company has more then 50 full-time investigators detecting and thwarting cheats. Bob Johnson, vice president of Bell Atlantic Mobile in the Washington/Baltimore region said, "We're quickly identifying cellular fraud and catching offenders, which has been a tremendous savings of money and time." He continued, "It's helping us to keep fraudulent calls from ever reaching customers' bills."

Nonetheless, keep your eyes open for any unusual calls or activity on that monthly bill. Another tell-tale sign someone may be fraudulently using your number is if you suddenly begin receiving lots of wrong number calls or hang up calls on your cellular phone. Call your carrier right away!

He stressed that customers won't be responsible for fraudulent calls, but "they do suffer the inconvenience of having to change their cellular telephone number if their phone has been cloned."

Using the latest intelligent software which analyzes calling patterns, an unusually high volume of calls and other tell-tale signs of cellular fraud, officials are getting tough with criminals. The goal is to nab the suspects at the onset, that's why it's important for the industry to work closely with law enforcement. Ed Kmiec, Bell Atlantic Mobile director of financial services and fraud management said, "Law officers' understanding of this relatively new crime, coupled with our ability to give the precise location of criminals, has led to swift apprehension of offenders." Not surprisingly too, cellular fraud is often just the tip of the criminal's iceberg.

CellularOne and its parent company McCaw Cellular Communications are developing innovative anti-fraud systems and taking numerous steps to detect and stop cellular fraud, including Fraud Protection Feature or FPF, which allows customers to lock service when not using their phone.

Also, by using a new software system they're examining cellular calls, looking at 17 call characteristics that's compared with the customer profile. If the information doesn't readily fit a usage profile it triggers the system and the subscriber is subsequently notified that fraud is suspected. Other techniques, including a pre-call verification feature, whereby a subscriber's ESN and MIN are validated prior to a call being delivered, are being used. This effectively eliminates tumbling fraud, according to McCaw and CellularOne. Additionally, digital authentication and even voice print technology are on the horizon to validate subscribers to curtail fraud.

These and other cellular companies are providing their customers with added security to thwart cellular fraud by providing customers with a personal identification number or PIN which is similar to an ATM code. During the dialing sequence, customers enter their private PIN number which provides an additional layer of calling security. For instance, early this year Bell Atlantic and NYNEX Mobile Communications began using a new Fraud Zone Protection Zone technique developed by Bell Atlantic Mobile. The program restricts calling throughout the greater New York City area for its customers from Washington, DC; Baltimore; Pittsburgh; and greater Philadelphia, including Delaware and southern New Jersey. Proper identification, along with a selected PIN code is required for those customers while roaming in New York City before the company will deactivate the fraud zone restriction.

It's a well-known fact (although you'd never believe lawmakers knew it when the ECPA was passed!) that cellphones are simple radio transmitters. It's also a fact that every phone, like each of us, has its own unique "fingerprint." A system that tracks, identifies and blocks illegally-made cellular

NEW! ScanStar™ Commercial Edition

From Signal Intelligence

The Leader In Computer Scanning

The Commercial Edition has all Professional features plus:

- Multi-radio scanning, search/slave & peer strategies.
- Spectacular graphical scan window has "all in vew" status. Quickly lock/unlock channels with mouse.
- Two independent scan windows. Scan up to 4 radios at the same time. Hot switch display.

Professional Edition Features:

- Spectrum analysis on R7100, R9000, AR3000, OS456, NRD535. Great graphics - support for most printers.
- Scan by tone with OS456 or DC440 + other radio.
- Scan multiple groups, banks and search ranges all at the same time! Alarms for priority channels.
- Unlimited channels and banks. Select all features on a per-channel basis. No frequency restrictions.
- Comprehensive report printing & data logging.
- Import & export data, read & write radio memory.
- Terminal window for TNC, decoder or modem.
- Monitoring Assistant, background scan & more!

Equipment Supported:

OS456, R7100, R7000, R9000, FRG9600, DC440, AR3000, NRD535, NRD525, R8, MR8100.

System Requirements:

IBM PC 386/486/586 with 4 MEG ram, hard disk, VGA, mouse, serial ports. DOS 5/6 with DOS=HIGH, or OS/2 2.1 or 3.0. Cables and interfaces not supplied.

Commercial Edition $129.97

Professional Edition $79.97

Plus shipping, handling and state sales taxes. To order call.

1-408-926-5630

Signal Intelligence
PO BOX 640891
San Jose CA 95164
408-926-5630
VOICE & FAX

FREE DEMO

Download from Scan*Star BBS, 2400-9600 N81, login as "guest"

1-408-258-6462

CIRCLE 77 ON READER SERVICE CARD

GMRS EMERGENCY Radios

- Hiking
- Fishing
- Skiing
- Camping
- Traveling
- Hunting

Communicate with others NOW using the most versatile radio available on the market today.

MAXON

GMRS-210+3

2-5 Watt portable

NOW Only $ 210.00

(Comes with the nationwide emergency frequency, 462.675 MHz installed!)

Many other accessories are available: headsets, mobile antennas, speaker/mics and more. Mobile radios too!

GMRS RADIO SALES

P. O. Box 37825

Phoenix, AZ 85069

1-800-571-GMRS

Fax: (602) 878-6398

CIRCLE 63 ON READER SERVICE CARD

calls is used in deterring cellular fraud. Let's suppose an illegal cellular user has a cloned phone and dials that long distance number. Instantly, the system identifies the signal pattern for the calling phone. If it doesn't match the one on file, the call is terminated.

Blocking a caller's initial access is the goal of the transmitter fingerprinting process. This method of fraud control is having remarkable results, according to Mr. Bill Taliaferro of Corsair Communications, a Sunnyvale, California-based company that develops and provides technology-intensive applications and solutions for the wireless industry. Known by the trade name PhonePrint, this fraud control system detects illegal phones by measuring in real time the unique characteristics of each phone's radio signal. The new system can determine if the call is from a legitimate caller. If not, it automatically blocks the clone's access to the cellular network. The company emphasizes that the PhonePrint system eliminates the need for users to change phone numbers when fraud is detected, and increases cellular network capacity by eliminating illegal traffic.

Don Winters, director of technology transfer at AirTouch Communications, which has partnered with the PhonePrint folks said, "This pre-call validation allows us to keep criminals off our network which in turn reduces costs incurred by fraud and increases capacity for our paying customers to use the AirTouch network." Operational deployment of the system in Los Angeles is the first major sale of the system by Corsair Communications.

A pleasant chat could cost you plenty if your number is stolen or cloned, then used by others to run up huge overseas toll calls.

The cellular fraud epidemic can be slowed down, with everyone's help. Here's what you can do.

•Your subscriber agreement, which includes your electronic serial and mobile telephone number, should be treated like any other sensitive personal document. You wouldn't expose your credit card numbers and agreements for the world to see, would you? Keep it in a safe place!

•Take your phone with you or store it in a locked area when leaving your vehicle, especially in an isolated area.

•Report your stolen phone to your cellular phone carried immediately.

•Remove your cellular antenna, lock the phone (or remove the handset) before leaving your vehicle with parking attendants, repair shops, etc. Maybe you should also consider buying that magnetic-mount antenna instead of the on-glass you now have.

•Why have long distance or overseas calling on your plan if you don't intend to use them? Ask your service provider to eliminate this long distance service.

•Use reputable cellular service technicians to install and test your phone.

Cellular fraud, as one company official said, "is not a victimless crime." After all, those costs have to be passed along to someone.

* * *

A special thanks to Bob Hagen, a reporter with WINS Radio, New York City, for providing some of the information used in developing this article. ■

BUY SMART

SG-230 Smartuner®

Antenna Coupler

SSB, AM, CW & DATA

You can't buy a smarter tuner than this. An automatic antenna coupler so intelligent it precisely tunes any length antenna -8 to 80 ft-in the HF band.

The Smartuner® automatically evaluates and switches 64 input and 32 output capacitance combinations, plus 256 inductance combinations in a "pi" network. The amazing result is over a half-million different ways to ensure a perfect match for your transceiver. And the most intelligent feature of all is that the Smartuner remembers the chosen frequency and tuning values, and will automatically reselect those values-in less than 10 ms, each time you transmit on that frequency.

The SG-230 Smartuner.® Buy smart.

MICROPROCESSOR CONTROLLED • NON-VOLATILE MEMORY • WATERPROOF
B.I.T.E. INDICATOR • 1.8 TO 30 MHZ RANGE
3 TO 150 WATTS INPUT POWER • 10mS RETUNING TIME • 8 to 80 ft. ANTENNA (all types)

SGC

NO COMPROMISE COMMUNICATIONS

800-259-7331

MADE IN USA

SGC, INC. SGC BUILDING P.O. BOX 3526 BELLEVUE, WA 98009 TEL. (206) 746-6310 FAX: (206) 746-6384

CIRCLE 75 ON READER SERVICE CARD